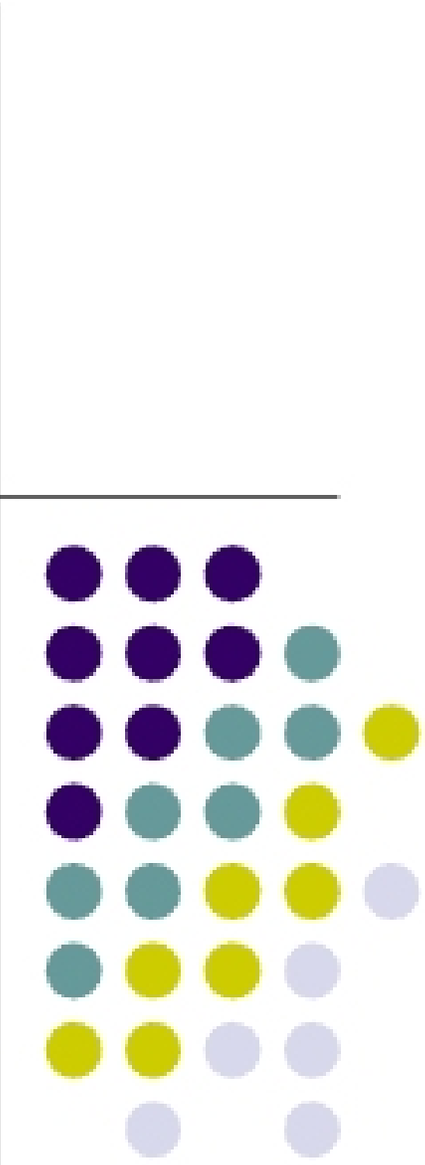
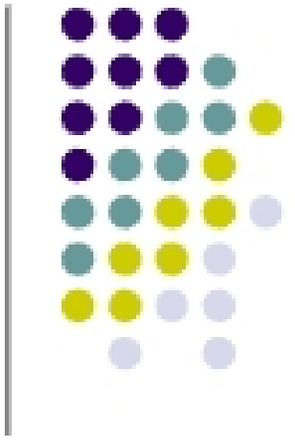
CSCI 530L



Public Key Infrastructure

Who are we talking to?



- Problem: We receive an e-mail. How do we know who it's from?
  - E-Mail address
    - Can be spoofed easily
  - E-Mail Header
    - Most of it can be spoofed, but not all of it
    - Pain to go through all the information
  - Call the person, and ask them if they sent it
    - If you received the e-mail at 3:00 PM PDT, and the guy is in India, it's 3:00 AM there.

Solution

- We should have a way of verifying, in the e-mail, who it is really from
  - Digital Signature
    - Uniquely verifies that a sender has sent the document, similar to a real signature
    - Takes a hash of the message – digest
    - Encrypts the digest using the private key
    - Anyone who reads the e-mail can see the signature, decrypt it using the public key, and if the digest matches the message, then this user sent the message